3. fejezet

Elrettentés a kibertérben: elérhető cél vagy ábránd?

Nyáry Gábor

Bevezetés

2021 forró nyara több szempontból is megrázta a világot. Az Egyesült Államok visszahúzódása Közép-Ázsiából, megtetézve Afganisztán villámgyors összeomlásával alapvetően új helyzetet teremtett a geopolitikában. A 21. századi konnektivitás, az új selyemút fő sodorvonalában található térség politikai, hatalmi viszonyainak alakulása természetszerű hatással van a globális erőtér sorsának alakulására. Ilyenformán ez az eseménysor közvetlenül kapcsolódik a multipolárisnak nevezett új világrend formálódásához. Van azonban a drámai átalakulásnak egy másik, közvetett kapcsolódási pontja is a geopolitikai struktúrák világához. A kelet-ázsiai térség regionális erőviszonyainak átalakulása mellett az afganisztáni összeomlásnak egy másik, messzire ható következménye is érzékelhető: ez az amerikai kredibilitás drámai megrendülése. Szövetséges és rivális egyaránt arról beszél: a mód, ahogyan az USA „lezárta" a két évtizedes afganisztáni térnyerését, alapjaiban kérdőjelezi meg az ország nagyhatalmi szerepvállalásának hitelességét.

Szokatlannak tűnhet, hogy egy meglehetősen specifikus téma – a kibertér elrettentési stratégiái és gyakorlatai – tudományos vizsgálata ilyen aktuálpolitikai felütéssel kezdődjön. Az ok prózai: ez a világesemény ékesszólóan mutatja az elrettentésproblematika legfontosabb összefüggését és meghatározó kulcsmozzanatát.[1]

Mindenekelőtt fontosnak tartjuk az elrettentés problémaköre vizsgálatánál a kontextus „becsületének" visszaállítását. Ez alapvető szempont a jelenség egyes részleteinek, illetve az elrettentési téma egészének megértéséhez. Világosan látnunk

[1] Plauzibilis feltételezésnek tekinthető ráadásul az is, hogy ez az eseménysor, éppen e két jellemzője (az átfogó geopolitikai erőviszonyok módosítása, illetve az amerikai kredibilitás megtépázása révén) számottevő hatással lehet a kiberelrettentés koncepciójának alakulására. Ez érintheti az egyes nagyhatalmak kiberelrettentési stratégiáinak alakulását, illetve a terület két vezető hatalma, az USA és Oroszország között nemrégiben megindult bilaterális tárgyalásokat.

https://doi.org/10.36250/01079_03

https://orcid.org/0000-0003-4327-9550

kell: az elrettentés a kibertérben – paradox módon – nem valamiféle „kibertéma". A „kibertér" nem önmagában létező, tehát önmagában vizsgálható terület. Egy átfogó, valamennyi „hadszínteret" *(domént)* és valamennyi „fegyverrendszert" felölelő biztonságpolitikai mező egyik – bár kétségtelenül növekvő fontosságú – szelete. Ennek megfelelően a kibertér nemzetbiztonsági célú használatára és kezelésére vonatkozó koncepciók is részei egy átfogó, a nemzetbiztonság valamennyi aspektusát érintő gondolkodásnak. Nem kivétel ez alól a kiberelrettentés témaköre: a vele kapcsolatos elméletek, stratégiák, operatív politikák és alkalmazási mechanikák tekintetében egyaránt. A nemzetbiztonsági, geopolitikai kontextus tehát meghatározó a kiberelrettentés vizsgálatánál.[2]

Az elrettentés kérdéseinek tanulmányozásánál feltűnő ugyanakkor az, hogy a nemzetközi szakmai közvélemény egy jókora része erősen technikai jellegű problémaként tekint erre az ügyre. A kiberelrettentés ennek megfelelően sokszor információtechnológiai vagy éppen játékelméleti szakproblémaként tűnik fel. Természetesen a kérdés sok (egyebek mellett erősen technikai jellegű) területet is érint. Legfontosabb jellemzője azonban a „nem technikai", tehát alapvetően humán jellege. Ha úgy tetszik: a kiberelrettentés vizsgálata sokkal inkább a pszichológusok, semmint a mérnökök terepe. A téma legkiválóbb kutatói nem mulasztják el hangsúlyozni: az elrettentés (a kibertérben éppen úgy, mint a többi hagyományos és új doménben) tulajdonképpen percepciós kérdés. Kulcsa az emberi mozzanat: az, hogy emberek (akik nemzeteket képviselnek ebben a játszmában) hogyan érzékelik a világot, annak veszélyeit, lehetőségeit és szükségességeit. Az elrettentés egyik legfontosabb eleme, tényezője nem véletlenül: a hitelesség, a hihetőség, tehát a kredibilitás. A holisztikus perspektíva és a lélektani elem egybefonódva szolgálja vagy gátolja az elrettentés mechanikáját. A valamelyik másik területen hitel nélküli vagy kredibilitását vesztett ellenfél a kibertér zugaiban is csak korlátozottan érvényesítheti elrettentési szándékát.[3]

[2] Ezt a holisztikus szemléletet szeretnénk hangsúlyozni a tanulmány más pontjain is: a terminológia kérdéseinek vizsgálatakor éppen úgy, mint az intervenciós eszközcsoportok bemutatásánál. Mindenhol aláhúzva, kidomborítva azt az álláspontot, amely szerint az „elrettentésként" ismert és használt koncepció valójában a nemzetek közötti stratégiai stabilitás témakörének egy szelete csupán. A gondolat jó összegzését adja a geopolitika egyik legjelesebb kutatója. Colin S. Gray: Geopolitics and Deterrence. *Comparative Strategy,* 31. (2012), 4. 295–321.

[3] John Stone: Conventional Deterrence and the Challenge of Credibility. *Contemporary Security Policy,* 33. (2012a), 12. 108–123.

Elrettentés vagy valami más? A fogalmi keretek használhatósága

Láthatjuk, már a téma exponálásának kezdetén kerülgetnünk kell bizonyos fogalmakat. Ideje, hogy egy kicsit elidőzzünk a terminológia problémájánál. Ebben az esetben ugyanis a szó köznapi értelmében is problematikus kérdéssel találjuk szembe magunkat. A tudományos kutatás, publikálás szokványos és indokolt eljárása, hogy a munka elején rögzítjük, definiáljuk a későbbiekben használni kívánt fogalmakat és kifejezéseket. A kiberelrettentés tanulmányozása azonban már itt, az első lépéseknél nagy akadályokat gördít elénk.[4] Olyannyira, hogy – a szokásos gyakorlattól eltérően – ebben a fejezetben nem kíséreljük meg átfogó keretrendszerként leírni, pontosan definiálni a témához kapcsolódó szavakat és fogalmakat. Itt tehát csupán arra szorítkozunk, hogy felvessük, bemutassuk a kiberelrettentés problémakörének elemzésekor felvetődő terminológiai problémákat. Úgy ítéljük meg, hogy az egyes fogalmak használatos (vagy általunk javasolt, használhatónak gondolt) elnevezéseit a későbbiekben, a fejezet egyes témaköreihez kapcsolódóan jobban, plasztikusabban, indokolhatóbban tudjuk majd magyarázni.

Az „elrettentés" fogalma ugyanis a maga nemében különös: egyszerre világos, plasztikus, nagy kifejező erőt mozgósító, ráadásul közérthető és közhasználatú kifejezés.[5] Másrészt viszont erősen félrevezető a szó használata. A helyzet röviden az (ahogyan arra a későbbiekben még részletesen kitérünk), hogy szinte az elrettentés koncepciójának megjelenésétől kezdve ez a kifejezés („elrettentés")[6] vált közkeletűvé, közhasználatúvá, és ez így is maradt napjainkig. Annak ellenére történt ez így, hogy időközben – a téma elméleti kérdéseinek alapos és kiterjedt tanulmányozása, valamint a sikerrel alkalmazott gyakorlatok meghonosodása nyomán – az eredeti koncepció jelentősen kibővült.[7] A koncepció, a fogalom szintjén ugyanis arról van szó, hogy (a nemzetközi térben egymással kapcsolódó, súrlódó) államok valamilyen módon megpróbálják elérni, biztosítani, hogy riválisaik, ellenségeik ne lépjenek fel ellenük támadó módon. Kezdetben ezt a fenyegetésen alapuló

[4] Emilio Iasiello: Is Cyber Deterrence an Illusory Course of Action? *Journal of Strategic Security,* 7. (2021), 1. 55–67.

[5] Michael J. Mazarr: *Understanding Deterrence*. Santa Monica, RAND, 2018; valamint Patrick M. Morgan: *Deterrence. A Conceptual Analysis*. London, Sage Publications, 1977. A kutatás jelenlegi állásáról ad összegzést Patrick M. Morgan: The State of Deterrence in International Politics Today. *Contemporary Security Policy,* 33. (2012), 12. 85–107.

[6] Angolul *deterrence*.

[7] Stephen L. Quackenbush: *Understanding General Deterrence Theory and Application*. New York, Palgrave Macmillan, 2011.

„elrettentés" kívánta szolgálni: ennek keretében azt tudatosították ellenfelükben, hogy az esetleges agresszív, támadó lépések válaszlépést, megtorlást fognak kiváltani.[8] Az idők folyamán azonban kialakult egy másik mechanizmus is, amelynek lényege, hogy az ellenfélben azt tudatosítják, hogy nem érdemes agresszíven, támadóan fellépni, mert az akció úgysem lesz sikeres (a megelőző lépéseinknek hála). Ezt az intézkedési pillért a szakma – talán a bevált elnevezéshez ragaszkodva – szintén „elrettentésnek" kezdte nevezni, és az elrettentés két módozataként említette a két különböző eszköz alkalmazását.[9] Valójában azonban nagyon eltérő intervenciós eszközökről van itt szó, ahol nemcsak a technika, hanem az egész mögöttes lélektani háttér is drámaian különböző. Ezt a megközelítést célszerűbb volna „eltántorításnak"[10] nevezni, hangsúlyozva, hogy itt nem a fenyegetés a meghatározó mozzanat a célok elérésére. A szakirodalom ezt a két módozatot említi többnyire az „elrettentés" szokványos megközelítésmódjaként. A hidegháború időszakában azonban kialakult még egy további koncepcionális lehetőség az ellenfél támadó fellépésének megelőzésére. E mögött igen fontos elméleti-tudományos felismerés áll, amely aztán még ennél is nagyobb horderejű politikai alapelvben öltött formát. A tétel lényege: a támadó sokszor azért támad, mert úgy érzi, hogy nem maradt számára más lehetőség érdekei képviseletére vagy védelmére. Ebből következően a támadó, ellenséges magatartás meggátolására nemcsak a megtorlással való fenyegetés vagy az akció kilátástalanságának bizonygatása szolgálhat, hanem az: meggyőzni az ellenfelet, hogy szükségtelen, indokolatlan az agresszív fellépése. Ezt a megoldást talán az „okafogyottság bizonyításának" lehetne nevezni.

Jól látható tehát, hogy valójában az „elrettentés" kifejezés használatakor ma már egy jóval átfogóbb koncepcióra gondolunk: amiről itt valójában szó van, az a „stratégiai stabilitás keresése". Az egyes (egymással szemben álló) államok[11]

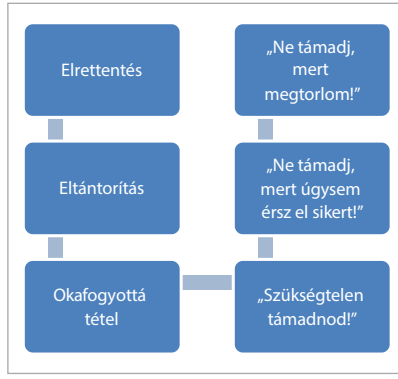
[8] Aihito Yamashita: Glenn Snyder's Deterrence Theory and NATO's Deterrence Strategy during the Cold War. *Air Power Studies,* 6. (2020). 69–116.; valamint Satoshi Yamamoto: On Thomas Schelling's Deterrence Theory. *Air Power Studies,* 6. (2020). 117–144.

[9] Martin C. Libicki: *Cyberdeterrence and Cyberwar.* Santa Monica, RAND Air Force Project, 2009; valamint Martin C. Libicki: Expectations of Cyber Deterrence. *Strategic Studies Quarterly,* 12. (2018), 4.

[10] Az angol szakmai nyelv az utóbbi időben lassan elkezdte erre az intézkedéscsoportra a *dissuasion* kifejezést használni a korábban általános *deterrence* helyett.

[11] Itt szeretnénk megjegyezni: a szakirodalomban és a szakmai gondolkodásban az elrettentés, így tehát a kiberelrettentés is alapvetően az államközi kapcsolatok jelenségeként tűnik fel. Ahol tehát egy szuverén állam próbálja meg stratégiai stabilitását biztosítani egy másik szuverén állami szereplővel kapcsolatban. A valóságban azonban az elrettentés problémája – különösen a kibertér világában – egyre gyakrabban merül fel nem állami szereplőkkel összefüggésben is. A 2021-es

ezt a stabilitást különböző megközelítésmódok alkalmazásával kísérelhetik meg biztosítani. A stratégiai stabilitást garantálni hivatott három alapvető mechanizmus demonstratív ábráját az *1. ábrán* látható formában lehet megrajzolni (ne feledjük, hogy ezt a három módszert, megközelítést osztatlanul „elrettentésnek" nevezi a szakirodalom túlnyomó része):



1. ábra: Törekvések a stratégiai stabilitás biztosítására
Forrás: a szerző szerkesztése

A hatalmi politika furcsa paradoxona: miközben a szakemberek egyöntetű meggyőződése az, hogy a fenyegetés, a tulajdonképpeni „elrettentés" a stratégiai stabilitás biztosításának legkevésbé sikeres módszere (és az esetleges támadás sikertelenségét garantáló megközelítés, de főleg a támadó fellépést eleve megelőző perspektíva a legeredményesebb), mégis ez a legelterjedtebb megközelítés a kibertérben is.[12]

év nagy „újdonsága", hogy kiberbűnözői csoportok akciói immár nemzetbiztonsági fenyegetést jelentenek szuverén államok számára. A kiberelrettentés lehetőségeit ezért egyre gyakrabban fogják a nem szuverén államok közötti, de nemzetközi kapcsolatrendszer kontextusában vizsgálni.

[12] Azzal a megjegyzéssel, hogy ezen a téren bizonyos lassú elmozdulás jelei éppen mostanában érzékelhetőek, elsősorban a meghatározó szereplőnek tekinthető USA vonatkozásában, ahogy arra a későbbiekben még utalni fogunk.

Emlékek a múltból: a hidegháború és a nukleáris elrettentés

Az „elrettentés”,[13] annak mindhárom fentebb bemutatott módozata valószínűleg ősi, és bizonyára egyidős az egymás mellett élésre kényszerülő emberi közösségekkel (a „közösségközi” konfliktusokkal, háborúkkal).[14] Jelen témánk szempontjából ezért a múlt tapasztalatainak feltérképezését arra a korszakra érdemes korlátozni, amelyben az elrettentés kérdéskörének tudományos igényű vizsgálata és leírása megkezdődött, majd szárba szökkent. Ez a tudomány- és politikatörténeti kutatóút a hidegháború időszakába vezet minket vissza.[15]

Az elrettentéssel kapcsolatos kérdések vizsgálatában, az ahhoz kapcsolódó elméletek alapjainak kidolgozásában az amerikai tudományos élet tagjai játszottak kiemelkedő szerepet, különösen Thomas Schelling, akinek a munkássága korszakalkotónak bizonyult ezen a területen.[16] A közgazdász végzettségű Schelling, aki tudományos pályafutása mellett számos meghatározó kormánytanácsadói posztot is betöltött, a hidegháborús konfrontáció csúcspontján, 1960-ban publikálta első, meghatározó írását a „konfliktusviselkedés” témakörében.[17] Ez a munka (amelyet később a 20. század második fele egyik legbefolyásosabb tudományos alkotásaként aposztrofáltak) a „stratégiai viselkedés” és az államok közötti alkufolyamatok kérdéskörét vizsgálta. A könyvben lényegében lefektette az elrettentés elméleti vizsgálatának számos fogalmi alapját. Néhány évre rá, eredeti gondolatait továbbfejlesztve, újabb korszakos írásban fejtette ki immár az elrettentés elvi lehetőségeinek szinte minden fontos elemét.[18] Munkásságának (amelyet a kor olyan drámai válsághelyzeteihez kapcsolódó kormányzati döntésekre alapozva fogalmazott meg, mint a berlini válság vagy a kubai atomrakéta-krízis) legfontosabb mondandója

[13] Noha már látjuk, hogy az „elrettentés” kifejezés helyett indokoltabb volna más, inkluzívabb terminust (mint amilyen például a stratégiai stabilitás keresése) alkalmazni. Ugyanakkor az „elrettentés” kifejezés az elmúlt fél évszázad szakmai és politikai szóhasználatában annyira meggyökeresedett, hogy a helyesebb kifejezésre váltás súlyos konfúzióhoz vezethetne. Ezért a szövegben mi is szinonimaként használjuk majd e szót.

[14] Robert P. Haffa Jr.: The Future of Conventional Deterrence: Strategies for Great Power Competition. *Strategic Studies Quarterly,* 12. (2018), 4. 94–115.

[15] Temi Davis Biddle: Coercion Theory: A Basic Introduction for Practitioners. *Texas National Security Review,* 3. (2020), 2. 94–109.

[16] Robert Ayson: *Thomas Schelling and the Nuclear Age. Strategy as Social Science*. London, Frank Cass, 2004.

[17] Thomas C. Schelling: *The Strategy of Conflict*. Cambridge, Harvard University, 1960.

[18] Thomas C. Schelling: *Arms and Influence: with a New Preface and Afterword*. New Haven, Yale University Press, 1966.

az volt, hogy a katonai erőnek, a primér erőszakos alkalmazásán túl, az államok közötti alkufolyamatokban is fontos szerep juthat az erőegyensúly-állapotok kialakításában és garantálásában.

Schelling és a nyomában járó amerikai társadalomtudós-nemzedék fogalmazta meg az államok közötti nyílt összecsapások megelőzésére, megakadályozására szolgáló elrettentési stratégiák számos nélkülözhetetlen elemét, illetve kellékét.

Ekkor jelenik meg a tudományos közgondolkodásban az elrettentés két lehetséges megközelítése (a tulajdonképpeni elrettentés, a *deterrence,* és a megakadályozás, amelyet ekkor a *denial* kifejezéssel illetnek), azok specifikumaival, sajátos feltételeivel és mechanizmusaival.[19] Érdemes megjegyezni: a kor viszonyai természetesen alapvetően befolyásolták a tudományos közgondolkodást, ami az elrettentéssel foglalkozó szakemberek esetében is jól érzékelhető. A 20. század közepe a roppant pusztító erejű nukleáris arzenálok kiépülésének kora, így érthető módon az offenzív megközelítések domináltak mindkét nagyhatalom stratégiai elképzeléseiben. Ennek megfelelően ebben az időben a megtorlással való fenyegetésre épülő elrettentés koncepciója, illetve stratégiája vitte a prímet.[20]

William Kaufmann érdeme volt annak a felismerése, hogy a sikeres elrettentés csak olyan stratégia köré épülhet, amely egyszerre tartalmazza az ellenfél elleni csapáshoz szükséges kapacitásokat és az erőszakos (válasz-) csapással kapcsolatos szándékot (eltökéltséget).[21] A felismerés lényege ugyanis az volt, hogy az elrettentés működéséhez elengedhetetlen, hogy a szemben álló felet meggyőzzük arról, hogy tartózkodjon az agresszív fellépéstől.[22] Thomas Schelling ezt azzal a fontos kitétellel fejelte meg, hogy a sikeres elrettentésnek lényeges eleme továbbá az is, hogy egy ellenséges fellépés nyomán alkalmazott megtorlás következményeit, illetve a válaszlépésre való elszántságot világosan kommunikálni kell a potenciális agresszor felé. A téma klasszikusai (különösen Schelling) már bő fél évszázada világosan megfogalmazták tehát a jó (hatásos, eredményes) elrettentési stratégia

[19] A tulajdonképpeni elnevezés ekkor még *deterrence by punishment,* azaz a megtorlás fenyegetésével való elrettentés, illetve a *deterrence by denial,* azaz a megakadályozás kilátásba helyezésével való elrettentés. Az egyik első klasszikusnál: Glenn H. Snyder: Deterrence and power. *The Journal of Conflict Resolution,* 4. (1960), 2. 163–178.

[20] Alexander L. George – Richard Smoke: *Deterrence in American Foreign Policy: Theory and Practice.* New York, Columbia University Press, 1974.

[21] William Kauffman: The Requirements of Deterrence. In P. Bobbitt et al. (szerk.): *US Nuclear Strategy.* London, Palgrave Macmillan, 1989.

[22] Krista Langeland – Derek Grossman: *Tailoring Deterrence for China in Space*. Santa Monica, RAND, 2021.

lényegét – ami azonban a mai napig gyakran elkerüli a témával foglalkozók figyelmét. A jó elrettentési stratégia tulajdonképpen nem „elrettenti" (a várható súlyos megtorlással) vagy „eltántorítja" (az akció megakadályozásával) az ellenfelet. Hanem elhiteti az ellenféllel, hogy képesek vagyunk a megtorlásra vagy a cselekvés megakadályozására – és azt meg is fogjuk tenni.[23]

Érdemes röviden megjegyezni: a hidegháború időszakában, amely egyben az atomfegyverkezés hajnala is volt, szinte kezdettől nyilvánvalóvá vált, hogy az elrettentés stratégiái és mechanizmusai máshogy működhetnek a hagyományos fegyverekkel, illetve az atomképességekkel kapcsolatosan.[24] Első pillantásra a nukleáris fegyverzet ideális elrettentő „fedezetnek" tűnhetett; valójában, éppen a totális pusztítást hozó jellege miatt, kevéssé volt alkalmas (ugyanis nem számított hihető fenyegetésnek) a megtorlásra épülő elrettentés eszközeként.[25] A hagyományos fegyverzet, amely nagy erejű, ám mégis korlátozott pusztítást garantált, sokkal hatékonyabbnak bizonyult a válaszcsapással fenyegető megelőzés szempontjából.

Üzenet a jövőből: elrettentés a világűrben

A kiberelrettentés kérdéseinek vizsgálatánál érdekes támpontokat, gondolati pilléreket biztosíthat egy másik *domén,* a világűr speciális elrettentési tematikája.[26] A világűr – hasonlóan a föld, víz, levegő térhármasához – szintén természetes közeg, ellentétben az egyértelműen ember alkotta kibertér világával. Ugyanakkor az űr jelentősen eltérő sajátosságokat mutat, és ilyenformán hasznos analógiákat kínálhat a kiberelrettentés szempontjainak tanulmányozásához.[27]

[23] Langeland–Grossman (2021): i. m.

[24] James J. Wirtz: How Does Nuclear Deterrence Differ from Conventional Deterrence? *Strategic Studies Quarterly,* 12. (2018), 4. 58–75.

[25] Joseph S. Nye Jr.: Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly,* 5. (2011), 4. 18–38.

[26] Noha a világűr mint a jelentős hatalmak közötti békés (és kevésbé ártatlan) vetélkedés színtere legalább 1957 óta jelen van a globális konfliktusmezők rendszerében, és a 20. század hidegháborús évtizedeinek zömében kiélezett „űrverseny" zajlott a Szovjetunió és az USA között, az elrettentés problematikája szempontjából csupán mostanában nő meg a jelentősége. A világűrbeli elrettentés elméleti alapozása ezért csaknem párhuzamosan folyik a kiberelrettentés teóriáinak kimunkálásával.

[27] Az egyik legelgondolkodtatóbb munka a témáról: Bleddyn E. Bowen: From the Sea to Outer Space: The Command of Space as the Foundation of Spacepower Theory. *Journal of Strategic*

Az első fontos megállapítás a világűr nemzetbiztonsági jelentőségére vonatkozik.[28] Kétség sem fér hozzá, hogy az elmúlt évtizedek fejlesztései nyomán az űr olyan rendszerek telepítési és működési területévé változott, amelyek ma már nélkülözhetetlenek a modern társadalmak működéséhez. A műholdas helymeghatározó rendszerektől a banki adatforgalmat bonyolító adatátviteli hálózatokig a modern társadalmak szinte minden artériája a világűrön fut keresztül. Az ott telepített rendszerek minden szempontból kritikus infrastruktúrát jelentenek.[29]

Az egyik legfontosabb megfigyelés, elméleti alapvetés az űrelrettentés átfogó jellegére vonatkozik.[30] Valójában nem is maga a konfrontáció színteréül szolgáló *domén* a lényeg, hanem a célpont jellege. Itt nem a fegyver az elsődleges, hanem a célpont milyensége. Egyszerű, de plasztikus és érvényes analógiával élve: a kibervilágban egy nagy adatközpont elleni robbantásos (tehát nem kibernetikai, hanem abszolút hagyományos „kinetikus") támadás éppen olyan drámai hatásokkal járhat, mint ha egy zsaroló vírusos támadás blokkolja az adatbázisokhoz való hozzáférést. Ez a nézőpont persze már eleve jelzi a célpontok milyenségéből eredő különbségtétel fontosságát: ahogy egészen más fenyegetést jelent egy Planet Lab kereskedelmi fényképező műhold blokkolása békeidőben, mint egy amerikai Keyhole nemzeti felderítő műhold megbénítása válságidőszakban, éppen annyira különbözik a felhasználók véletlenszerű csoportjai elleni primitív zsaroló vírusos támadás egy nagy energiaelosztó cég szervereinek megbénításától.

Az űrelrettentés érdekes sajátossága – megint egy használható analógia – az, hogy olyan (állami és nem állami) aktorok is támadhatnak űreszközöket, amelyek maguk nem rendelkeznek hasonló képességekkel. A válaszcsapás, illetve az azzal való fenyegetés tehát nem lehet szimmetrikus.[31] Ez világosan mutatja, hogy a korszerű (űr-, illetve kiber-) elrettentés mindenképpen több doménre kiterjedő megtorlással fenyegetve hatásos.[32]

A nukleáris hadviseléshez (válaszcsapáshoz) kapcsolódó űrrendszerek sérülékenysége különleges jelentőségű, a hozzájuk kötődő elrettentési stratégiának ezt

Studies, 42. (2019), 3–4. 532–556.

[28] Forrest E. Morgan: *Deterrence and First-Strike Stability in Space. A Preliminary Assessment*. Santa Monica, RAND Air Force Project, 2010.

[29] Dean Cheng – John Klein: A Comprehensive Approach to Space Deterrence. *The Strategy Bridge,* 2021. március 31.

[30] Langeland–Grossman (2021): i. m.

[31] Bleddyn E. Bowen: The Art of Space Deterrence. *European Leadership Network,* 2018. február 20.

[32] James P. Finch: Finding Space in Deterrence: Toward a General Framework for „Space Deterrence". *Strategic Studies Quarterly,* 5. (2011), 4. 10–17.

figyelembe kell vennie.[33] Újfent egy hasznos, elgondolkodtató analógia a kibertér viszonyaira vetítve.

Az űreszközök (műholdak) egy része, támadás esetén, érzékeny, de nem életbe vágó fontosságú veszteséget jelenthet civil használók tömegeinek. Ilyen esetekben viszonylag gyenge a fenyegetéshez kapcsolódó érzelmi és politikai töltés, ami a kapcsolódó elrettentés eredményességét csökkentheti.[34]

Bizonyos űrtámadások (az általuk okozott kiterjedt létfenyegetés miatt) olyan erősen eszkalatórikus jellegűek (hasonlóan a nukleáris arzenálokhoz), hogy az kétségessé teszi azok alkalmazhatóságát, s így a hozzájuk kapcsolható elrettentő potenciál is viszonylag csekély.[35]

A kibertér sajátos világa

A földrajzi tér alapvető kiterjedései, a szárazföldek és a vizek ősidőktől az államok közötti érdekérvényesítési küzdelmek állandó színterei. Melléjük a 20. század első harmadától felzárkózott a levegő, majd a hidegháború korszakában az űr dimenziója is. A 21. század újdonságaként ez a sokrétű geopolitikai világ újabb versengési területtel bővült ki. A formálódó kibertér lett a geopolitikai szembenállás, érdekérvényesítés ötödik dimenziója.[36] Az informatika, a számítógépes hálózatok, a mobiltechnológiák rohamos fejlődése szülte ezt az új „érdekmezőt", ebben az értelemben tehát tényleg ízig-vérig korunk terméke. Mint annyi fogalom, a „kibertér" is sok értelmezést, értelmezési árnyalatot takar.[37]

[33] Steve Lambakis: A Guide for Thinking About Space Deterrence and China. *Comparative Strategy,* 38. (2019), 6. 497–553.

[34] Michael Krepon – Julia Thompson (szerk.): *Anti-Satellite Weapons, Deterrence and Sino-American Space Relations.* Washington, Stimson, 2013.

[35] A világűrbeli elrettentés különösen érdekes körülményeként szokták említeni az óriási mennyiségben keletkező űrtörmelék szempontját. Az elmélet úgy szól, hogy az ellenfél űreszközének kinetikus (tehát nem informatikai, kibernetikai) megsemmisítése, az ennek eredményeként keletkező törmeléktömeg révén, a támadó fél rendszereire is óriási fenyegetést jelentene. Következésképpen ez erős visszatartó erővel bír (illetve jelentősen csökkenti az űrellencsapással való fenyegetés elrettentő erejét).

[36] A kibertér geopolitikai jellegének egyik első megfogalmazását Szilágyi István: *A geopolitika elmélete* című kiváló munkája adja (Budapest, Pallas Athéné, 2018).

[37] A kibertér sajátosságaihoz áttekintést ad Nyáry Gábor: Kiberdiplomácia: hatalom, politika és technológia a geopolitika ötödik dimenziójában. In Török Bernát (szerk.): *Információ- és kiber-*

A kifejezés nem új keletű: egy William Gibson nevű íróhoz kötődik, aki 1982-ben kiadott novellájában használta első ízben ezt a fordulatot, egy számítógép által kreált virtuális valóságmező bemutatására. Ma már az internet egész világot körbefonó, számítógépes hálózatainak szinonimájaként használatos. A kibertér „térbeli" mivoltával kapcsolatban a szakirodalom nem egységes. Egyes szerzők, különösen a kiberhadviselés problematikájával foglalkozó stratégiatudományi szakértők a sokdimenziós geopolitikai közeg fokozatos virtualizálódásáról beszélnek. E szerint a hagyományos tereket a csupán átvitt értelemben létező, konkrét alakot nélkülöző tér, egyfajta „térnélküliség" váltja a geopolitika összefüggésrendszerében.[38]

Másfelől viszont a kiberkomplexum technológiai aspektusaival vagy a digitalizáció társadalmi összefüggéseivel foglalkozó kutatóknál hangsúlyosan merül fel a kibertér térjellege, azaz nagyon is valóságos, fizikai térstruktúrákhoz integránsan kapcsolódó mivolta. Ebben a felfogásban a kibertérfogalom térbelisége különböző szinteken jelenik meg. A fogalomnak elsőként is van egy technikai jelentésszintje, amely a kibertérnek nevezett fogalom együttes technológiai infrastruktúráját írja le. A fogalomnak van ugyanakkor egy tényleges földrajzi jelentésrétege is, amely az IKT-hálózatokat és azok csomópontjainak valóságos térbeni kiterjedését öleli fel. Ugyanakkor tartalmaz egy harmadik, társadalmi jelentésréteget is, amely az IKT-hálózatokat használó emberek térbeli szerveződéseit írja körül. A kibertér, ez a sokszor virtuálisnak nevezett világ tehát nagyon is valóságos térbeliséggel rendelkezik.

Komplex jellege magyarázza, hogy a kibertér miért számít speciális közegnek az elrettentés stratégiái szempontjából is. A teljesség igénye nélkül érdemes emlékeztetni néhány fontos specifikumra. A legfontosabb talán az, hogy a kibertér technológiai komponensei alapvetően kettős rendeltetésű elemekre épülnek. A polgári alkalmazást sokszor lehetetlen megkülönböztetni a támadó célú eszközöktől. Lényeges jellegzetesség az is, hogy a kibertérben folyó rosszindulatú műveletek olyan széles spektrum mentén zajlanak, amelyek sokszor nem érik el a „harci cselekménynek" minősülő konfliktusok határát. Emellett nehéz a támadó cselekmények észlelése, felderítése, ami értelemszerűen visszahat az elrettentés eredményességére is. A kibertérben mozgó ellenfelek igyekeznek az online terek

biztonság. Fenntartható biztonság és társadalmi környezet tanulmányok V. Budapest, Ludovika Egyetemi Kiadó, 2020. 321–343.

[38] Szilágyi István: *A geopolitika elmélete*. Budapest, Pallas Athéné, 2018.

sötétjében meghúzódni, ezért a próbálkozások, behatolások észlelése nem könnyű feladat.

A kibervilág legfontosabb sajátossága kétségtelenül az attribúció nehézsége.[39] A tettes egyértelmű azonosítása olyan vizsgálati folyamat, amelynek során kiberbiztonsági szakemberek bizonyító erejű információkat gyűjtenek, eseményidőrendeket állítanak össze, és mindezekből fáradságos munkával összerakják a hálózatot vagy gépet ért támadást. A tevékenység célja az, hogy bizonyítható módon megállapítsa, hogy ki volt egy-egy kiberakció végrehajtója, illetve ki lehet az, aki egy támadó akcióért a tényleges felelősséget viseli.[40]

Sokan állítják: az attribúció egyáltalán nem lehetetlen. Mindig sok olyan nyom marad egy-egy támadó akció után, amelyből aprólékos munkával összeállítható az elkövető képe. Ennek azonban ellentmondani látszik, hogy a szinte korlátlan erőforrásokkal és hatalmas tudáskapacitásokkal rendelkező hatalmak is csupán a legritkább esetben prezentálnak evidenciát egy-egy támadás feltételezett elkövetőjének megnevezésekor. Az attribúciók az esetek túlnyomó részében számos hipotetikus elemet tartalmaznak, illetve a bizonyító anyag ereje nézőpont kérdése, tehát jogilag korántsem egyértelmű.

Mechanizmusok és modellek

A kiberelrettentés lehetséges modelljének kialakításához, a digitális doménben is működőképes elrettentési stratégia bemutatásához érdemes egy pillantást vetni a hagyományos konfliktustér elrettentési mechanizmusára.

Az elrettentés elmélete és működése a hidegháború időszakában

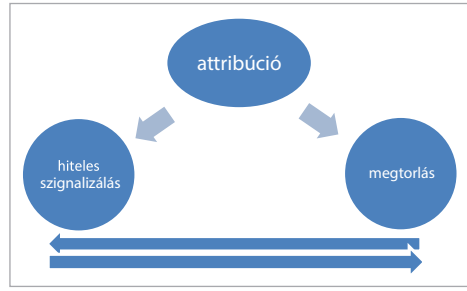
A téma egyik elismert kutatója, Mariarosariaria Taddeo sematikus összefoglalója ma már klasszikusnak számít az irodalomban.[41] Ebben – tehát a hagyományos

[39] Clara Assumpção: The Problem of Cyber Attribution Between States. *E-International Relations,* 2020. május 6. Átfogóan vizsgálja a problémát Will Goodman: Cyber Deterrence. Thougher in Theory than in Practice? *Strategic Studies Quarterly,* 4 (2010), 3. 102–135.

[40] Nicholas Tsagourias – Michael Farrell: Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law,* 31. (2020), 3. 1–27.

[41] Mariarosariaria Taddeo: *How to Deter in Cyberspace*. Strategic Analysis. Helsinki, Hybrid CoE, 2018b.

elrettentés viszonyrendszerében – kulcsszerepet kap az attribúció. Ez (legyen szó hagyományos vagy nukleáris fegyverzetről) nagyobb nehézségek nélkül érvényesíthető. Ezzel szemben – mint feljebb láttuk – a kibertér viszonyai között az attribúció roppant problematikus, és a hatékony elrettentés legfőbb akadálya.[42]



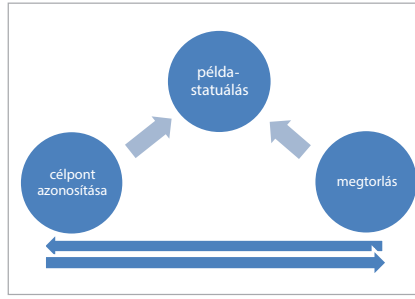
2. ábra: A hagyományos elrettentésmodell
Forrás: Taddeo (2018a): i. m.

Az ábra egyértelműen mutatja azt is: a szignalizáció (a képességek és az elszántság kommunikálása) az elrettentés másik fontos eleme. Taddeo azonban úgy véli, hogy a kibertér viszonyai között ez a létfontosságú jelzés is csupán tökéletlenül működhet. Egyszerűen azért, mert egy-egy állam „kiberreputációja" nem feltétlenül esik egybe tényleges kiberkapacitásaival (és ez utóbbit, mint az előző fejezetben utaltunk rá, gyakorta tartják az érdekelt felek homályban). A modell harmadik fontos összetevője, a megtorlás mind a hagyományos, mind pedig a kibertérségben jól működhet. A kiberdoménben azonban a megtorlás (tehát a kibertérben történő támadáshoz hasonlóan ugyanezen doménben történő válaszcsapás) rendkívüli kockázatokat rejt, a könnyű eszkalálódás lehetősége folytán.[43]

[42] Richard J. Harknett: Leaving Deterrence Behind: War-Fighting and National Cybersecurity. *Journal of Homeland Security and Emergency Management,* 7. (2010), 1. 1–24. Fontos elméleti alapvetést hoz továbbá Mariarosaria Taddeo: Deterrence and Norms to Foster Stability in Cyberspace. *Philosophy and Technology,* 31. (2018a), 4. 323–329.
[43] Alexander A. Ghionis: *The Limits of Deterrence in the Cyber World. An Analysis of Deterrence by Punishment*. Brighton, University of Sussex, (é. n.).

A kiberelrettentés lehetséges modellje

Taddeo hangsúlyozza: a kiberelrettentés koncepciójának kialakításánál fontos, hogy ne engedjünk a hagyományos elrettentésmodellek hamis analógiájának. A kibertér sajátosságai döntően befolyásolják a használható elrettentési stratégiát. Fontos emlékeznünk rá: a kibertér az állandó támadás terepe. A támadás taktikai és stratégiai értelemben egyaránt előnyösebb, mint a védekezés.[44]



3. ábra: A kiberelrettentés modellje
Forrás: Taddeo (2018a): i. m.

A kibertér sajátos viszonyaihoz alkalmazkodó, speciális elrettentési elmélet és stratégia kialakításánál Taddeo szokatlan és merész fordulattal azt javasolja: az attribúciót (a támadó hiteles megállapítását) ki kell hagyni az egyenletből. Helyette egy plauzibilis „célpont" azonosítására kell koncentrálni, amelyre a másik fő komponens, az ellencsapás (megtorlás) irányulhat. Így valósulhat meg az elrettentő erő demonstrálása.[45]

Az elmélet szerint, ha az azonosított (bár nem bizonyított) célpontra ellencsapást mérünk, akkor az eredeti támadó művelet így előidézett megszakítása jelenti majd a „bizonyítékot".[46] Ez a megközelítés azonban nem csupán roppant

[44] Taddeo (2018a): i. m. Ez a szemléletmód tükröződik abban a váltásban is, amely az USA kiberbiztonsági koncepcióját jellemzi. A klasszikus (passzív) védekezés egyre inkább átadja a helyét az (aktív) „előretolt védelem" szisztémájának.

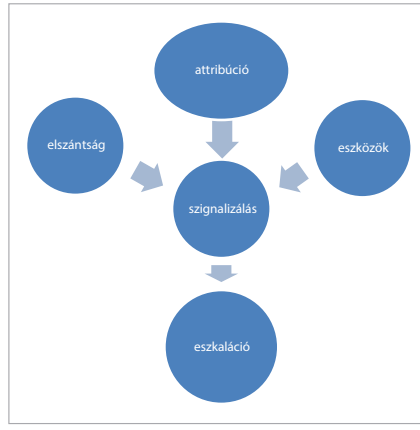
[45] További részleteket hoz Mariarosaria Taddeo: The Limits of Deterrence Theory in Cyberspace. *Philosophy and Technology,* 31. (2018c), 4. 323–329.

[46] Taddeo kétségtelenül szokatlan felvetése arra az állításra alapul, hogy manapság a támadó (akár a folyamatokat automatizáló gépi tanuló rendszerek segítségével) viszonylag jó hatékonysággal

kockázatos, de ráadásul tulajdonképpeni elrettentésre sem alkalmas. Legfeljebb csak egy „majdani" második támadás megelőzésére bizonyulhat használhatónak.

Az összefüggések jobb megértése felé

A fenti javaslat egyelőre csupán gondolatkísérletnek tekinthető, és mindenképpen érdemes mérlegre tenni egy ilyen megközelítés veszélyeit és sok szempontból beláthatatlan (nemzetközi jogi, etikai és természetesen politikai) következményeit.[47] Célszerű ugyanakkor egy sémában bemutatni a kibertérben megvalósítható (megtorlásra épülő, tehát „valódi") elrettentés fontos elemeit és azok összefüggésrendszerét.



4. ábra: Az elrettentés összefüggései a kibertérben
Forrás: a szerző szerkesztése

Az általunk vázolt modell a jelenleg alkalmazott rendszert demonstrálja. Egyértelmű szakmai igény mutatkozik arra, hogy az elrettentés rendszerét az egyes elemek hatékonyságának a növelésével dinamizálják.[48] Az egyik fő irány

azonosítható, „csupán" ennek bizonyítása ütközik nehézségbe. Érdemes azonban megfontolni: ez a „csupán" szócska az a hajszál, amely a jogállami normák érvényesüléséhez köt minket.

[47] Taddeo (2018b): i. m.

[48] Joseph Nye Jr.: Deterrence and Dissuasion in Cyberspace. *International Security,* 41. (2016–17), 3. 44–71. Összehasonlításként érdemes áttekinteni: Rod Thornton – Marina Miron: Deterring Rus-

nyilvánvalóan az attribúcióval kapcsolatos vizsgálati rendszer tökéletesítése (nem kis részben a mesterségesintelligencia-alapú technológiákra támaszkodva).[49] De nem ez a dolog kulcsa. Az általunk kiegészített modell – visszanyúlva az elrettentéselmélet klasszikusainak megállapításaihoz – azt kívánja demonstrálni, hogy az elrettentés, ahogy régebbi korokban és doménekben, úgy a mostani kibervalóságban sem technikai kérdés. Ennek megfelelően – hiszen valójában döntően percepciós kérdésről van szó – az igazi kulcs a szignalizáció hatékonyságának növelése lehet: a rendelkezésre álló erőforrások (hiteles) bemutatása, és az azok alkalmazására való készség demonstrálása.[50] A felrajzolt séma ugyanakkor rámutat az esetleges nem kívánatos kimenetelekre, a folyamatban rejlő inherens veszélyekre is. A kibertér sajátosságai ugyanis mindenképpen megnövelik a gyors és könnyű eszkalálódás veszélyét.[51]

Útkeresések, megoldási irányok

A kiberelrettentés hatékony stratégiájának kialakításánál érdemes visszakanyarodni ahhoz a kezdő gondolathoz, miszerint a tulajdonképpeni elrettentés csupán egy elem az államok stratégiai stabilitását biztosítani hivatott mechanizmusok között. Talán nem is a legfontosabb. Korábban rámutattunk: a hidegháború idején ténylegesen az offenzív fellépés, a fenyegetésre alapozott elrettentés volt a stabilitás vágyott kulcsa. Ugyanakkor abban is egyetértenek a szakértők, hogy ez a fenyegetés mindig is a legkevésbé hatékony biztonságteremtő eszköznek számított.[52] Célszerű lehet tehát, ha a stabilitás biztosítására hivatott eszközrendszeren belül a másik kettőre kerülne a hangsúly: a támadást értelmetlenné tevő, illetve a táma-

sian Cyber Warfare: The Practical, Legal and Ethical Constraints Faced by the United Kingdom. *Journal of Cyber Policy,* 4. (2019), 2. 257–274.

[49] Tim Stevens: A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy,* 33. (2012), 12. 148–170.

[50] Sico van der Meer: *Signalling as a Foreign Policy Instrument to Deter Cyber Agression by State Actors.* Hague, Clingendael, 2015.

[51] Jun Osawa: The Escalation of State Sponsored Cyberattacks and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pacific Review,* 24. (2017), 2. 113–131.

[52] Ehhez ad érdekes kiegészítést Eric Sterner: Retaliatory Deterrence in Cyberspace. *Strategic Studies Quarterly,* 5. (2011), 1. 62–80. A vezető kibernagyhatalom, az USA stratégiájába illesztve vizsgálja ugyanakkor ezt a kérdést Michael E. O'Hanlon: Deterrence. US Grand Strategy and the Wisdom of Bob Gates. *The Brookings Institution,* 2021. június 7.

dást feleslegessé tevő intézkedések erősítésére. Már csak azért is, mivel az elmúlt évtizedben mindkét területen fontos lépések történtek.

Felderítés, verifikálás: „nyitott kiberégbolt"

Mielőtt az agressziót értelmetlenné, illetve feleslegessé tevő megoldásokról ejtenénk szót, érdemes még egy pillanatra elidőzni egy olyan témánál, amely elsődlegesen a (fenyegetésen alapuló) elrettentés összefüggésében játszhat szerepet, ugyanakkor a stabilitás erősítését célzó teljes ökoszisztéma profitálhat az eredményeiből. A felderítés, az ellenfelek kölcsönös (intézményi keretek közt folyó) monitorozása, tehát az ellenfél kapacitásainak és szándékainak verifikálása minden stabilitást szolgáló intézkedéscsomagban kulcselemként jelenik meg. A helyzet egyik nagy paradoxona, hogy miközben a kiterjedt ellenséges kiberfelderítési akciók jelentik ma a globális hatalmak közötti feszültségek egyik forrását, a kibertér zavartalan működését biztosítani hivatott kiegyezések (kiberfegyverszünetek, kiberfegyverzet-korlátozási megállapodások) egyik sarokköve, megvalósításának záloga éppen a kölcsönös „felderítés" erősítése lehet. A hidegháború nukleáris krízishelyzeteit vizsgáló tanulmányok sora világított rá: a (kölcsönös) hírszerzés, természetesen bizonyos szabályozott keretek között, éppen a bizalmatlanság, egzisztenciális fenyegetettségérzet eloszlatásában játszott meghatározó szerepet. Később, az enyhülés szakaszában az úgynevezett „nyitott égbolt" megállapodással intézményesült ez a lehetőség. A nagyhatalmak közötti kibertér-megállapodások, bilaterális kezdeményezések egyik eleme lehet egy ehhez hasonló konstrukció kiépítése, amely az elrettentés többi mechanikája esetében is erősítheti a hatékonyságot.

Reziliencia

A stratégiai stabilitást biztosítani hivatott mechanizmusok között a második blokk, az „eltántorítás" konkrét eszközrendszere különböző elemeket ölel fel. Mindegyik arra szolgál, hogy megüzenje a potenciális agresszornak: nem érdemes támadnia, mert úgysem jár sikerrel. Idő- és ráfordításigényes védekezési mód, ám a kutatók egy része szerint messze eredményesebb a reziliencia növelése, mint a fenyege-

tések rendszere.[53] A reziliencia, az ellenálló képesség erősítése maga is többfajta intézkedést ölelhet fel: a rendszerek redundanciáinak fokozása (például a sebesen elharapódzó zsaroló vírusos támadások célpontjául szolgáló adatkészletek duplikálása) mellett az informatikai rendszereket és eszközöket használók biztonsági képzettségének növelésén át az egyszerű kiberhigiénés szabályok rutinszerű intézményesítéséig.

A SolarWinds-támadás mély nyomokat hagyott a kiberbiztonsági szakértőkben. Terjed az a koncepció, hogy alapvetően új védekezési eljárásokat és taktikát kell kidolgozni, mert bebizonyosodott, hogy az ellenfél hackerei „ott vannak már a legbelső védvonalakon belül". Ennek megfelelően az úgynevezett „zéró bizalom modell" olyan belső védelmi technológiákra támaszkodik, amelyek folyamatosan ellenőrzik, hogy egy adott eszköz, felhasználó vagy szoftver az elvárásoknak megfelelően működik-e (azaz nem került-e illetéktelen befolyás alá). Ez a koncepció élesen szakít az eddigi szokványos kiberbiztonsági filozófiával, amely a rendszerekbe való illetéktelen behatolások megakadályozására fókuszált.

Az állami rendszerek szintjén is változik a védekezésről vallott hagyományos koncepció. Mindez jól tükröződik az Egyesült Államok kibervédelmi intézményrendszerének változó stratégiájában, amely a hagyományos (periméteralapú, passzív jellegű) védekezésről a „folyamatos harcérintkezésen" alapuló, „előretolt kibervédelem" aktív megközelítésére helyezte át a hangsúlyt.[54]

Felelős viselkedés, kiegyezés: normák és alkuk

Sokan rámutattak már: az offenzív kiberműveletek hátterében az esetek többségében nem holmi gonoszság, hanem emberi félelem, a cselekvési kényszer képzete áll. Azaz: egy támadóan fellépő állami kiberszereplő mozgatórugói között sokszor az a meggyőződés áll az első helyen, hogy (nemzeti érdekei érvényesítéséhez vagy azok megvédéséhez) kénytelen támadóan fellépni. Ne feledjük a klasszikus elrettentéselmélet alapvető megállapítását, axiómáját: az emberi játszmák (köztük az államközi összecsapások) nem hidegen gondolkodó logikai gépek között folynak; az elrettentés problematikájának a gyökerében emberi percepciók, hiedelmek állnak. Ez az oka, hogy az „elrettentés" (tehát a stratégiai stabilitás biztosítása)

[53] Nathan Ryan: Five Kinds of Cyber Deterrence. *Philosophy and Technology,* 31. (2018), 2. 331–338.
[54] Emily O. Goldman: Fresh Thinking and New Approaches Are Needed on Diplomacy's Newest Frontier. *Foreign Service Journal,* 2021. június.

legeredményesebb eszköze az lehet, amely meggyőzi az ellenfelet arról, hogy nincs szüksége arra, hogy támadjon.[55]

Az „okafogyottá tétel" mechanizmusának legfontosabb, legjellemzőbb eszköze a tárgyalás, a megállapodás. Thomas Schelling az elrettentés teóriáját megalapozó fél évszázaddal ezelőtti művében figyelmeztet: az igazi erő az alkuerő. Kiaknázása pedig a diplomácia dolga. Az igazság az, hogy a nemzetközi kiberdiplomácia nem is tétlenkedett az elmúlt évtizedekben. A kibertér biztonságát, élhetőségét előmozdító szabályozórendszer kialakítása folyamatosan napirenden van az utóbbi két évtizedben. Szereplők egész sora feszült neki a kibertérben való mértékadó viselkedés normarendszere kialakításának.[56] A kollektív szabályozórendszer hagyományos eszköze, a nemzetközi jog alapvetően államok és állami eredetű szervezetek viszonyrendszerének rendezésére szolgál.[57] A kibertér egyik szembeötlő sajátossága azonban éppen a szereplők sokasága és sokfélesége. Ennek fényében nem csoda, hogy jogi kötéssel bíró eszköz egyetlen esetet – a kiberbűnözésről szóló budapesti konvenciót – leszámítva nem is született mindeddig. Inkább az irányelvnél átfogóbb, a kívánt viselkedéssel kapcsolatban egyértelműen fogalmazó, de a nemzetközi törvénnyel ellentétben nem kötelező erejű normarendszerek kidolgozása került a kibertér-szabályozó törekvések középpontjába. Figyelemre méltóak ebben a tekintetben az úgynevezett *Tallinni kézikönyvek,* amelyek szakértői összefogásból, önkéntes alapon születtek meg.

Az új évezred elején állította fel az ENSZ Közgyűlése az első úgynevezett kormányzati szakértői munkacsoportot (*Group of Governmental Experts* – GGE), hogy megvizsgálja az IKT-eszközök fejlődésének hatását a nemzetközi biztonság alakulására. Az elmúlt évtizedekben hat ilyen munkacsoport működött. Témájuk: a kibertérben való állami viselkedés kívánatos szabályainak, irányelveinek és normáinak kérdései; a nemzetközi szabályrendszerek érvényesülését segítő bizalomépítő intézkedések és kapacitásépítés. Részleges eredménytelenségek után a világszervezet normaalkotó szerepvállalásának dinamizálása érdekében egy új testület, a Nyílt végű Munkacsoport (OEWG) kezdte meg működését. Az ENSZ

[55] Timothy M. McKenzie: *Is Cyber Deterrence Possible?* Maxwell AFB, Air University Press, 2017. A nemzetközi közösséget átfogó normarendszereknek az elrettentésben betöltött hangsúlyos szerepére hívja fel a figyelmet Mariarosariaria Taddeo: Deterrence by Norms to Stop Interstate Cyber Attacks. *Minds and Machines,* 27. (2017). 387–392.

[56] Nyáry Gábor: Felelősségteljes állami viselkedés a kibertérben. Az ENSZ átfogó normaalkotó erőfeszítései. *Új Magyar Közigazgatás,* 14. (2021b), 3. 33–40.

[57] Christian Ruhl: *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at Crossroads.* Washington, Carnegie Endowment, 2020.

munkaszervezetei összességében nagyon fontos szerepet játszottak a kibertér szabályozottabbá tételében.

Az elrettentés elméletének kiemelkedő kutatói azonban már a 20. század második felében leszögezték, hogy a stratégiai stabilitásra irányuló valóban hatékony alkufolyamatok mindig egyedi jellegűek. Középpontjukban ugyanis valós emberek percepciói és félelmei állnak. Talán ez az oka annak, hogy a stabilitást célzó kollektív normarendszerek hatékonysága miért csekély. Ez különösen felértékeli az egyes hatalmak közötti bilaterális megegyezéseket. Az amerikai és orosz elnök közötti genfi csúcstalálkozó 2021 júniusában egyenesen korszakosnak nevezhető.[58] A hidegháború kezdete óta a szuperhatalmak egyezkedéseiben az atomfegyverkezés kérdései álltak a középpontban. Ez a mostani volt az első amerikai–orosz csúcstárgyalás, ahol a stratégiai stabilitás problémakörében alapvetően a kibertér viszonyai és fejleményei kerültek a fókuszba. Az ENSZ égisze alatt kidolgozott kiberszabályok fontos iránymutatást jelentenek – ám alapvetően önkéntesek, tehát jogi kötöttséggel nem járnak. Az amerikai–orosz csúcstalálkozó felvetése: egyetlen meghatározó témára kell fókuszálni az erőfeszítéseket, ám az így születő egyezségnek bilaterális, jogi érvénnyel kötelező megállapodási formát kell adni.[59]

A tárgyalások témáját a „célpontok korlátozásában" jelölték meg. Az elképzelés az, hogy a két állam abban állapodjon meg, hogy kölcsönösen tartózkodni fognak a jövőben egymás „kritikus polgári infrastruktúráinak" támadásától.[60] Az amerikai fél egészen szűkre szeretné szabni az egyeztetések fókuszát, és kizárólag a zsaroló vírusos kibertámadások megakadályozása-megelőzése szerepel a napirendjén. Az oroszok ugyanakkor ennél szélesebb kontextusban szeretnének megállapodást tető alá hozni. A tét nagy, hiszen a fenyegetésen alapuló hagyományos elrettentés alig működik a kibertérben. A bilaterális tárgyalással viszont esély nyílik a támadó fellépés kölcsönösen okafogyottá tételére.[61]

[58] Nyáry Gábor: A stratégiai stabilitás keresése. Amerikai–orosz kiberfegyverszüneti tárgyalások. *Ludovika Cyberblog,* 2021a. augusztus 5.

[59] *UNGGE Final Report 2019–2020*. New York, UNODA, 2021; valamint *OEWG Final Substantial Report*. New York, UNODA, 2021.

[60] Egy korábbi amerikai nézőpontot érdemes ezzel összevetni: Alex S. Wilner: Cyber Deterrence and Critical-Infrastructure Protection: Expectation, Application and Limitation. *Comparative Strategy,* 36. (2017), 4. 309–318.

[61] Alex S. Wilner: Us Cyber Deterrence: Practice Guiding Theory. *Journal of Strategic Studies,* 43. (2019), 2. 245–280.

Elágazások, további kutatási irányok

Az elrettentés problematikája a kibertérben egy különös benyomással gazdagítja a vizsgálódót. A téma kutatói (és ez elsősorban az elrettentés kérdéseinek elméleti részleteire fókuszálókat jelenti) szinte kivétel nélkül az államok közötti kapcsolatrendszer vonatkozásában veszik szemügyre az elrettentés, illetve a stratégiai stabilitást biztosító alkufolyamatok állapotát.[62] Eközben azonban a globális kibertér biztonsági környezete sebes tempóban alakul át, és ebben a transzformációban a koronavírus-világjárvány közel két esztendeje különösen markáns változásokat hozott. A kibertér, a számítógépes hálózatokat, a gépeket, a rajtuk futó szoftvereket és az őket használó embereket felölelő új társadalmi dimenzió rohamos gyorsasággal sötétül el a fölé boruló fenyegetésektől.[63] 2017-ben derült ki: a Yahoo cégtől 3 milliárd felhasználói adatelem jutott évekkel korábban illetéktelenekhez. 2018-ban az Equifax nevű amerikai hitelinformációs cég hálózatai váltak támadás áldozataivá, és mintegy 143 millió amerikai polgár személyes adatai kerültek ki a rendszerből. Még ugyanabban az évben jelentette a Marriott hotellánc, hogy 383 millió szállóvendégük adataihoz fértek hozzá illetéktelenek. Az elmúlt másfél évben szédületes növekedésnek indult (az esetszámokat és az eltulajdonított összegeket tekintve egyaránt) a zsaroló vírusos támadások „divatja": a nagy áttörést itt is a járványos 2020-as esztendő hozta meg a támadások meghétszereződésével. A kiberbűnözés esetszámai, a támadások súlya, a károkozás mértéke egyértelműen növekvő tendenciát mutat.

A zsaroló vírusos akciók egyre inkább a modern társadalmak (elsősorban az Egyesült Államok) alapvető működési rendjét biztosító hálózatokat, a legszorosabban vett társadalmi kritikus infrastruktúrát veszik célba. 2021 nyarára a helyzet súlyosbodása nyomán az amerikai kormányzat a nemzetközi terrorizmussal azonos súlyú fenyegetésnek minősítette az informatikai hálózatok és adatbankok zsaroló

[62] Ebben a tekintetben a néhány eddig publikált vállalati kutatás jelenti az egyedüli támpontot. Kiemelkedően magas elméleti színvonalon tárgyalja a kibertérben működő magánszereplőkkel szembeni elrettentés témakörét az egyik jelentős tanácsadó cég közelmúltban megjelent tanulmánya: Jesse Goldhammer et al.: *Leading the Way With an Adversary Focus. Government's Role in Deterring Cyber Attacks.* London, Deloitte, 2021. Különleges esetet vizsgál Thomas Rid: Deterrence Beyond the State: The Israeli Experience.*Contemporary Security Policy,* 33. (2012), 12. 124–147. munkája, amely a terrorszervezetek elrettentésének kérdésére fókuszált. Ehhez kapcsolódik, de a hagyományos doménekben: John Gearson: Deterring Conventional Terrorism: From Punishment to Denial and Resilience. *Contemporary Security Policy,* 33. (2017), 1. 171–198.

[63] Nyáry (2021b): i. m.

vírusokkal történő megtámadását. A nem kormányzati kiberszereplők (bűnözői csoportok) által végrehajtott támadások immár nemzetbiztonsági fenyegetéssel érnek fel a világ leghatalmasabb államában is.

Ez a drámai változás arra mutat, hogy az elrettentés problematikájának vizsgálatában egyfajta elágazáshoz értek a kutatók. A hagyományos – állami szereplőkre fókuszáló – témafelvetés mellett külön fejezetet szükséges nyitni a nem állami kiberaktorok elrettentésének is.[64] A csekély számú korábbi kutatás alapján máris jól látható, hogy az elrettentés valamennyi eddigi elméleti modellje (és az azokra épülő konkrét intézkedések és eszközök) újragondolandók. A magánszereplők által végrehajtott, közvetlenül más magánentitásokat vagy állami intézményeket érő, de nemzetbiztonsági súlyú kiberakciók elrettentésére a korábban alkalmazott megközelítések némelyike aligha működhet.[65] Nyilvánvaló az is: a jogi keretek drasztikus átalakítása (új jogszabályok alkotása, speciális bilaterális jogsegélyrendszerek kialakítása) nélkül nehéz lesz eredményesen szembeszállni ezzel a kihívással.[66] A probléma pedig végképp komplex megközelítést követel majd, ha a nem állami csoportok a világűr eszközeinek kiberrendszereit veszik célba.

Irodalomjegyzék

Általános elmélet és hagyományos elrettentés:

Ayson, Robert: *Thomas Schelling and the Nuclear Age. Strategy as Social Science*. London, Frank Cass, 2004.

[64] Eugenio Lilli: Redefining Deterrence in Cyberspace: Private Sector Contribution to National Strategies of Cyber Deterrence. *Contemporary Security Policy,* 42. (2021), 2. 163–188.

[65] Itt elsősorban az államok közötti viszonyrendszerben a legnagyobb eredményességgel kecsegtető „okafogyottá tétel" az, ami bűnözőkkel kapcsolatban nem jöhet szóba. A fenyegetésen alapuló elrettentés pedig még a hagyományos (hidegháborús) viszonyoknál is kevesebb eredményességgel kecsegtet ebben a közegben. Ugyanakkor az „eltántorítás" számos eszköze (zéró bizalom alapú védelem, reziliencia erősítése, felhasználói kiberhigiéné erősítése) jól használhatónak látszik a szervezett kiberbűnözői közeggel szemben is. A téma érdekes exponálását adja Elisabeth Braw – Gary Brown: Personalised Deterrence of Cyber Agression. *The RUSI Journal,* 165. (2020), 2. 48–54. A nemzetbiztonsági szempontból egyre képlékenyebbé, világos határokat nélkülözővé váló kibertér különös „ügyszövetségeiről", magán- és állami aktorok összefogásáról különösen érdekes perspektívákat vázol fel Herbert Lin – Amy Zegart: *Bytes*, *Bombs and Spyes. The Strategic Dimensions of Offensive Cyber Operations*. Washington, Brookings Institution, 2018.

[66] Duncan Hollis: *A Brief Primer on International Law and Cyberspace*. Washington, Carnegie Endowment, 2021.

Biddle, Tami Davis: Coercion Theory: A Basic Introduction for Practitioners. *Texas National Security Review,* 3. (2020), 2. 94–109. Online: http://dx.doi.org/10.26153/tsw/8864

George, Alexander L. – Richard Smoke: *Deterrence in American Foreign Policy: Theory and Practice.* New York, Columbia University Press, 1974.

Gray, Colin S.: Geopolitics and Deterrence. *Comparative Strategy,* 31. (2012), 4. 295–321. Online: https://doi.org/10.1080/01495933.2012.711116

Haffa, Robert P. Jr.: The Future of Conventional Deterrence: Strategies for Great Power Competition. *Strategic Studies Quarterly,* 12. (2018), 4. 94–115.

Kauffman, William: The Requirements of Deterrence. In Philip Bobbitt – Lawrence Freedman – Gregory F. Treverton (szerk.): *US Nuclear Strategy.* London, Palgrave Macmillan, 1989.

Mazarr, Michael J.: *Understanding Deterrence*. Santa Monica, RAND, 2018.

Morgan, Patrick M.: *Deterrence. A Conceptual Analysis*. London, Sage Publications, 1977.

Morgan, Patrick M.: The State of Deterrence in International Politics Today. *Contemporary Security Policy,* 33. (2012), 12. 85–107. Online: https://doi.org/10.1080/13523260.2012.659589

Quackenbush, Stephen L.: *Understanding General Deterrence Theory and Application*. New York, Palgrave Macmillan, 2011.

Rid, Thomas: Deterrence Beyond the State: The Israeli Experience. *Contemporary Security Policy,* 33. (2012), 12. 124–147. Online: https://doi.org/10.1080/13523260.2012.659593

Schelling, Thomas C.: *The Strategy of Conflict*. Cambridge, Harvard University, 1980.

Schelling, Thomas C.: *Arms and Influence: with a New Preface and Afterword*. New Haven, Yale University Press, 2008.

Snyder, Glenn H.: Deterrence and power. *The Journal of Conflict Resolution,* 4. (1960), 2. 163–178.

Stone, John: Conventional Deterrence and the Challenge of Credibility. *Contemporary Security Policy,* 33. (2012), 12. 108–123. Online: https://doi.org/10.1080/13523260.2012.659591

Wirtz, James J.: How Does Nuclear Deterrence Differ from Conventional Deterrence? *Strategic Studies Quarterly,* 12. (2018), 4. 58–75.

Yamashita, Aihito: Glenn Snyder's Deterrence Theory and NATO's Deterrence Strategy during the Cold War. *Air Power Studies,* 6. (2020). 69–116.

Yamamoto, Satoshi: On Thomas Schelling's Deterrence Theory. *Air Power Studies,* 6. (2020). 117–144.

Elrettentés a világűrben:

Bowen, Bleddyn: The Art of Space Deterrence. *European Leadership Network,* 2018. február 20. Online: www.europeanleadershipnetwork.org/commentary/the-art-of-space-deterrence/

Bowen, Bleddyn E.: From the Sea to Outer Space: The Command of Space as the Foundation of Spacepower Theory. *Journal of Strategic Studies,* 42. (2019), 3–4. 532–556. Online: https://doi.org/10.1080/01402390.2017.1293531

Cheng, Dean – John Klein: A Comprehensive Approach to Space Deterrence. *Strategy Bridge,* 2021. március 31. Online: https://thestrategybridge.org/the-bridge/2021/03/31/a-comprehensive-approach-to-space-deterrence

Finch, James P.: Finding Space in Deterrence: Toward a General Framework for „Space Deterrence". *Strategic Studies Quarterly,* 5. (2011), 4. 10–17.

Krepon, Michael – Julia Thompson (szerk.): *Anti-Satellite Weapons, Deterrence and Sino-American Space Relations.* Washington, Stimson, 2013.

Langeland, Krista – Derek Grossman: *Tailoring Deterrence for China in Space.* Santa Monica, RAND, 2021.

Lambakis, Steve: A Guide for Thinking About Space Deterrence and China. *Comparative Strategy,* 38. (2019), 6. 497–553. https://doi.org/10.1080/01495933.2019.1674081

Morgan, Forrest E.: *Deterrence and First-Strike Stability in Space. A Preliminary Assessment*. Santa Monica, RAND Air Force Project, 2010.

Kibertér és elrettentés:

Assumpção, Clara: The Problem of Cyber Attribution Between States. *E-International Relations,* 2020. május 6. Online: www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/

Braw, Elisabeth – Gary Brown: Personalised Deterrence of Cyber Agression. *The RUSI Journal,* 165. (2020), 2. 48–54. Online: https://doi.org/10.1080/03071847.2020.1740493

Gearson, John: Deterring Conventional Terrorism: From Punishment to Denial and Resilience. *Contemporary Security Policy,* 33. (2017), 1. 171–198. Online: https://doi.org/10.1080/13523260.2012.659600

Ghionis, A. Alexander: *The Limits of Deterrence in the Cyber World. An Analysis of Deterrence by Punishment.* Brighton, University of Sussex, é. n.

Goldhammer, Jesse – Joe Mariani – Matt Stapleton – Akash Keyal: *Leading the Way With an Adversary Focus. Government's Role in Deterring Cyber Attacks.* London, Deloitte, 2021. Online: www2.deloitte.com/za/en/insights/industry/public-sector/government-deter-cybersecurity-adversary.html

Goldman, Emily O.: Fresh Thinking and New Approaches Are Needed on Diplomacy's Newest Frontier. *Foreign Service Journal,* 2021. június. Online: https://afsa.org/cyber-diplomacy-strategic-competition

Goodman, Will: Cyber Deterrence. Tougher in Theory than in Practice? *Strategic Studies Quarterly,* 4. (2010), 3. 102–135.

Harknett, Richard J.: Leaving Deterrence Behind: War-Fighting and National Cybersecurity. *Journal of Homeland Security and Emergency Management,* 7. (2010), 1. 1–24.

Hollis, Duncan: *A Brief Primer on International Law and Cyberspace*. Washington, Carnegie Endowment, 2021.

Iasiello, Emilio: Is Cyber Deterrence an Illusory Course of Action? *Journal of Strategic Security,* 7. (2021), 1. 55–67. Online: http://dx.doi.org/10.5038/1944-0472.7.1.5

Libicki, Martin C.: *Cyberdeterrence and Cyberwar.* Santa Monica, RAND Air Force Project, 2009.

Libicki, Martin C.: Expectations of Cyber Deterrence. *Strategic Studies Quarterly,* 12. (2018), 4.

Lilli, Eugenio: Redefining Deterrence in Cyberspace: Private Sector Contribution to National Strategies of Cyber Deterrence. *Contemporary Security Policy,* 42. (2021), 2. 163–188. Online: https://188. doi.org/10.1080/13523260.2021.1882812

Lin, Herbert – Amy Zegart (szerk.): *Bytes, Bombs, and Spies. The Strategic Dimensions of Offensive Cyber Operations*. Washington, Brookings Institution, 2018.

McKenzie, Timothy M.: *Is Cyber Deterrence Possible?* Maxwell AFB, Air University Press, 2017.

Nyáry Gábor: A stratégiai stabilitás keresése. Amerikai–orosz kiberfegyverszüneti tárgyalások. *Ludovika Cyberblog,* 2021a. augusztus 5. Online: www.ludovika.hu/blogok/cyberblog/2021/08/05/a-strategiai-stabilitas-keresese/

Nyáry Gábor: Felelősségteljes állami viselkedés a kibertérben. Az ENSZ átfogó normaalkotó erőfeszítései. *Új Magyar Közigazgatás,* 14. (2021b), 3. 33–40.

Nyáry Gábor: Kiberdiplomácia: hatalom, politika és technológia a geopolitika ötödik dimenziójában. In Török Bernát (szerk.): *Információ- és kiberbiztonság. Fenntartható biztonság és társadalmi környezet tanulmányok V.* Budapest, Ludovika Egyetemi Kiadó, 2020. 321–343.

Nye, Joseph S. Jr.: Deterrence and Dissuasion in Cyberspace. *International Security,* 41. (2016–17), 3. 44–71. Online: https://doi.org/10.1162/ISEC_a_00266

Nye, Joseph S. Jr.: Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly,* 5. (2011), 4. 18–38.

OEWG Final Substantial Report. New York, UNODA, 2021.

Osawa, Jun: The Escalation of State Sponsored Cyberattacks and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pacific Review,* 24. (2017), 2. 113–131. Online: https://doi.org/10.1080/13439006.2017.1406703

Ruhl, Christian: *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at Crossroads.* Washington, Carnegie Endowment, 2020.

Ryan, Nathan: Five Kinds of Cyber Deterrence. *Philosophy and Technology,* 31. (2018), 2. 331–338. Online: https://doi.org/10.1007/s13347-016-0251-1

Sterner, Eric: Retaliatory Deterrence in Cyberspace. *Strategic Studies Quarterly,* 5. (2011), 1. 62–80. Online: www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-1/Sterner.pdf

Stevens, Tim: A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy,* 33. (2012), 12. 148–170. Online: https://doi.org/10.1080/13523260.2012.659597

Stevenson, Jonathan: Cyber Conflict and Deterrence. *Strategic Comments,* 22. (2016), 7. Online: https://doi.org/10.1080/13567888.2016.1237761

Szilágyi István: *A geopolitika elmélete*. Budapest, Pallas Athéné, 2018.

Taddeo, Mariarosaria: Deterrence by Norms to Stop Interstate Cyber Attacks. *Minds and Machines,* 27. (2017). 387–392. Online: https://doi.org/10.1007/s11023-017-9446-1

Taddeo, Mariarosaria: Deterrence and Norms to Foster Stability in Cyberspace. *Philosophy and Technology,* 31. (2018a), 3. 323–329. Online: https://doi.org/10.1007/s13347-018-0328-0

Taddeo, Mariarosaria: *How to Deter in Cyberspace.* Strategic Analysis. Helsinki, Hybrid CoE, 2018b.

Taddeo, Mariarosaria: The Limits of Deterrence Theory in Cyberspace. *Philosophy and Technology,* 31. (2018c), 4. 323–329. Online: https://doi.org/10.1007/s13347-017-0290-2

Thornton, Rod – Marina Miron: Deterring Russian Cyber Warfare: The Practical, Legal and Ethical Constraints Faced by the United Kingdom. *Journal of Cyber Policy,* 4. (2019), 2. 257–274. Online: https://doi.org/10.1080/23738871.2019.1640757

Tsagourias, Nicholas – Michael Farrell: Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law,* 31. (2020), 3. 1–27. Online: https://doi.org/10.1093/ejil/chaa057

UNGGE Final Report 2019-2020. New York, UNODA, 2021.

Van der Meer, Sico: *Signalling as a Foreign Policy Instrument to Deter Cyber Agression by State Actors.* Hague, Clingendael, 2015.

Wilner, Alex S.: Cyber Deterrence and Critical-Infrastructure Protection: Expectation, Application and Limitation. *Comparative Strategy,* 36. (2017), 4. 309–318. https://doi.org/10.1080/01495933.2017.1361202

Wilner, Alex S.: Us Cyber Deterrence: Practice Guiding Theory. *Journal of Strategic Studies,* 43. (2019), 2. 245–280. Online: https://doi.org/10.1080/01402390.2018.1563779